MARITIME SECURITY POSES UNIQUE CHALLENGES FOR GLOBAL COMMERCE

By Gerald P. Fleming

Other than national defense, the Coast Guard's missions historically have been largely domestic in scope with a focus on search and rescue, pollution control, and law enforcement. As a result of the events of September 11, counterterrorism and security were added to the Coast Guard's responsibilities, competing for limited resources to meet the mandates. With the struggle to assess the security in our domestic ports yet to be completed, the deadline of July 1, 2004, for international ports to comply with the International Ship and Port Facility Security (ISPS) Code is on the horizon.

Nature of the Problem

Ports have historically been open to ensure the free flow of commerce. The seas have been known throughout history to bring freedom and prosperity. For the United States, 95 percent of trade is waterborne and carried through our seaports, accounting for over 2 billion tons of cargo each year. Waterborne commerce is also expected to more than double in the next 20 years. Ports are diverse in size and operation, generally have open accessibility to both land and water, are linked to all modes of transportation, and many times are near large city

U.S. Coast Guard photo

Department of Defense photo

Opposite page: Currently, 95 percent of the United States' trade is waterborne and carried through our seaports, accounting for over 2 billion tons of cargo each year. Here, two ships are worked at the Port of Seattle's Terminal 18. Above and right: The October 2000 attack on the guided-missile destroyer USS *Cole* ushered in a new era in the maritime world – an era in which the possibility of a terrorist attack must always be considered. Above, a crewman onboard a 41-foot U.S. Coast Guard utility boat stands by as the USS *Cole*, following its extensive repairs, prepares to get underway in Pascagoula, Miss., in April 2002. The port side view at right shows the damage sustained by the USS *Cole* after a terrorist bomb exploded during a refueling operation in the port of Aden, Yemen.

centers. Historically, our ports have not been closely regulated, again because of the need to ensure the free flow of commerce.

The events of September 11 caused the international community to take a hard look at securing maritime commerce, both on ships and in ports. Note that the attacks in New York were directed at economic targets and symbols of world trade. One of the biggest lessons of the USS *Cole* incident is that the threat facing the maritime world today has changed dramatically. Each year, the U.S. marine transportation system transports over 6.5 million passengers, handles over 1 billion tons of petroleum, and has 7,500 ship arrivals. We have 95,000 miles of coastline and 361 public seaports. All told, our Marine Transportation System contributes over $1 trillion to the U.S. gross domestic product. The point is that the terrorist threat is not going away; it will become more challenging to address as world trade volumes grow. The Marine Transportation System was designed to move cargo with a minimum amount of delay, not around security principles. The fact that much of the Marine Transportation System works on "just in time" delivery presents an added challenge.

It is pretty self-evident to all nations that the Marine Transportation System is vital; it is the lifeblood of domestic and international commerce, and thus it is worth protecting. However, because maritime commerce is an inherently global venture, it is also evident that we must have an international solution. In order to maximize uniformity and predictability, ships should not be subject to differing requirements at different ports. Inconsistency can lead to imbalance between ports, with ships likely to seek those ports that impose only minimal requirements so that costs are minimized. This is an imbalance that cannot be tolerated. Security must be improved across the board, but it must be improved consistently.

The Challenges

In an effort to codify and standardize a comprehensive approach to effective, consistent international maritime security, the U.S. Coast Guard, in its role as the Department of Homeland Security's lead agency for maritime security, led efforts within the International Maritime Organization (IMO) to develop the International Ship and Port Facility Security (ISPS) Code. The ISPS Code, adopted by an IMO diplomatic conference in December 2002 as an amendment to the International Convention on the Safety of Life at Sea, is the only internationally accepted blueprint for the implementation of security measures for the maritime infrastructure. The Code has an entry-into-force date of July 1, 2004.

At the same time, Congress enacted the Maritime Transportation Security Act (MTSA). As a result, and because the security situation associated with foreign ports and vessels can have a direct impact on the security of the United States, the MTSA enacted sections 70108-70110 of Title 46 United States Code that require the Coast Guard to assess the effectiveness of antiterrorism measures implemented in foreign ports served by U.S. documented vessels from which foreign vessels depart on a voyage to the United States, and any other foreign ports the secretary believes pose a security risk to international maritime commerce.

The ISPS Code is a major step toward achieving our domestic and international goals. It was the product of very difficult negotiations after September 11, but over 100 nations came together in the spirit of unity and cooperation to develop what is considered to be a landmark international instrument, because the ISPS Code moved from concept to reality in just over a year's time – something remarkable for international negotiations. What is even more remarkable is the breadth of detail in the ISPS Code as compared to the traditional IMO instruments that historically were written as general obligations and broad regulations.

Moreover, the ISPS Code marks the first time that IMO really considered requirements related to port facilities. Most traditional IMO instruments focused on ship requirements. The ISPS Code focuses on the ship-port interface, or, in other words, the actions that occur when movement of people and goods, or provision of port services to or from the ship, directly and immediately affect a ship.

Photo courtesy of the Port of Seattle

A container ship is loaded at the Port of Seattle's Terminal 5.

The International Ship and Port Facility Security Code – Vessels

The ISPS Code is comprised of two parts. Part A is mandatory, and Part B contains the guidelines that must be taken into account in complying with Part A. Part A contains performance-based standards for both ships and port facilities. Part B is the roadmap for complying with Part A. Part B outlines the various measures that can be implemented for each performance standard in Part A. Ships and port facilities are free to choose one or a combination of the measures listed in Part B for each performance standard. If not choosing one of these measures, the ship or port facility must implement a measure that imposes an equivalent level of security. Although Part B is discretionary, it is an integral part of the code and it would be difficult to meet the requirements in Part A without using Part B as the roadmap to compliance. It must be noted that last year, the Maritime Safety Committee of IMO adopted a circular stating that Part B is a process that all parties had to go through in order to comply with Part A. With respect to ships, the committee further required that a certificate of compliance should not be issued until Part B had been taken into account. In other words, a ship or port facility would not be considered compliant unless it had also fully taken into account Part B of the ISPS Code.

The ISPS Code is actually an instrument that was developed as part of a new Chapter XI-2, titled "Enhanced Measures for Maritime Security," to the 1974 International Safety of Life at Sea Convention (SOLAS). Chapter XI-2 was adopted as an amendment to SOLAS by the diplomatic conference in December 2002. It is Chapter XI-2 of SOLAS that makes the ISPS Code applicable for all states that are a contracting government to SOLAS. Chapter XI-2 and the ISPS Code are amendments to SOLAS, and parties to SOLAS are automatically bound by the amendment. Fortunately, SOLAS happens to be one of the most – if not the most – ratified treaty in IMO's portfolio, and perhaps in the entire United Nations system. SOLAS has 147 parties, representing over 98 percent of the world's tonnage. Therefore, most of the world, including the United States, will comply with these new maritime security requirements. The ISPS Code enters into force on July 1, 2004. There is no phase-in period. On that date, ships and port facilities must fully comply with its provisions.

The International Ship and Port Facility Security Code – Ports

The ISPS Code applies to port facilities engaged in international trade. Therefore, a port facility that serves only ships in domestic trade is not subject to the ISPS Code, but should be separated sufficiently from other port facilities that do have to comply, such

The figures for the United States' waterborne commerce are growing. In the next 20 years, waterborne commerce is expected to more than double.

that these purely domestic port facilities do not present a risk of contaminating ISPS Code port facilities.

A port facility is a location, determined by the contracting government, where the ship/port interface takes place. There are two important points. First, the contracting government has discretion to define the parameters and boundaries of port facilities within its territories, provided it covers those locations and terminals that serve ships on international voyages. Secondly, the definition of a port facility in the ISPS Code expressly includes anchorages, waiting berths, and seaward approaches. This was the result of a compromise between those countries that wanted the ISPS Code to apply to all activities within the port and those that wanted to focus on the security of individual terminals serving ships. Therefore, what constitutes a port facility for the United States and a foreign port may differ. The common element must be, however, that measures are put in place to ensure the security of the ship-port interface.

Security Assessments

The ISPS Code requires that security assessments be completed as a first step in securing port facilities. A security assessment can cover more than one port facility, provided it fulfills the ISPS Code standard for security assessments. A port facility security plan must then be developed that details the specific measures that the port facility will implement. A port facility security officer must also be designated for the port facility, but the same port facility security officer can be designated for one or more port facilities. The port facility security officer is an important designation, because that person shoulders most of the responsibility for ensuring that the ISPS Code requirements are met and maintained by the port facility.

The ISPS Code also requires port facilities to conduct periodic training, drills, and exercises. Drills should be conducted every three months and be designed to test each element within the security plan. Exercises should be conducted once each calendar year, with no more than 18 months between exercises. They can also be held in combination with other emergency response or port authority exercises. The exercises should be coordinated with ships and shipping companies and may include full-scale or live exercises, table-top simulations, or seminars.

The U.S. Coast Guard has developed a Port Security Risk Assessment Tool that outlines the security assessment process. It also includes various matrices to help in categorizing risks and prioritizing assets and infrastructure. The Transportation Security Administration has developed a Web-based risk assessment tool (http://www.tsa.gov/public/display?content=0900051980064 0c8) that many in U.S. industry have found helpful with the vulnerability assessment element of the larger security assessment.

After the security assessment is completed, a report must be generated that contains the results of the assessment. The security assessment must be periodically reviewed and updated. In addition, it should be reviewed every time major changes to the port facility occur.

Security Plans

The security plan must be based on the results of the port facility security assessment. The plan must describe the operational and physical security measures that will be implemented at three escalating security levels. At a minimum, the security plan must address the following elements for each security level:

- It must describe the security organization of the port facility, including the assignment of security duties and responsibilities of personnel at the port facility.
- For access control, the plan needs to prescribe measures sufficient to prevent the entry of unauthorized persons and to prevent the introduction of weapons and other dangerous substances and devices.
- The plan needs to designate restricted areas.
- The plan needs to describe the measures for the security of cargo handling and the delivery of stores.
- Lastly, the plan must address security monitoring.

Port State Control

The new international maritime security requirements include a robust port state control regime. Port states, based on clear grounds that a ship is not in compliance with the ISPS Code, may delay or detain that ship, expel it from port, or deny it entry into the port.

The term "clear grounds" is not a significantly high standard of proof; it will be based on the totality of information available to the port state control officer and is effectively a matter of discretion. However, in a departure from traditional IMO practice, clear grounds in the security context can exist for conditions external to the ship itself. For example, if the ship called at a port facility that did not comply with the ISPS Code, that ship may be subjected to port state control at its next port of call, including the possibility of being denied entry. The ship may be required to describe what additional security measures it took while at the noncompliant port facility to mitigate the risk of a security incident. This is a major economic incentive for port

facilities to fully comply with the ISPS Code. If ships call on a particular port facility that is noncompliant and are routinely subject to port state control at subsequent locations, then those ships may no longer call at that port facility. As we all know, ships hate delays, and any delay in cargo operations or ship transits can be very expensive.

The port state control regime in the ISPS Code preserves the rights of states to take any necessary action under international law.

U.S. Approach to Other Nations' International Compliance and the ISPS Code

From an international perspective, the Coast Guard approach will be to promote a bilateral information exchange to align and share security practices and to increase maritime stakeholder awareness about the provisions of the MTSA. Through its International Port Security Program, the Coast Guard's goal will be to encourage bilateral and multilateral meetings and visits to exchange security-related information and to share best practices to harmonize port security programs.

The United States' approach to the ISPS Code is actually a combination of the ISPS Code and the International Labour Organization (ILO) Code of Practice. In fact, the U.S. Coast Guard's guidelines on port security were adopted by the Joint Groups of Experts at ILO as a best practice and used as a model for the Code of Practice.

For purposes of the U.S. domestic regime, each Coast Guard Captain of the Port Area is a port facility for purposes of the ISPS Code. As such and under the MTSA, the Captain of the Port, as the Federal Maritime Security Coordinator (FMSC), is the Port Facility Security Officer for ISPS. The port area security assessment is conducted by local port stakeholders who assist the FMSC in developing an area security plan. The exception to this is that the United States has designated 55 of its ports as strategic ports, meaning that they have some vital national security, defense, or economic significance. For these 55 strategic ports, a team of Coast Guard personnel will conduct the assessments, most of which will likely be classified and protected as national security information.

The area security plan will address all the core ISPS requirements across the FMSC area. Individual terminal and facility security plans will support the area security plan. In doing so, the U.S. Coast Guard, because of duties under the MTSA, has imposed security requirements on terminals and facilities beyond what the ISPS Code requires by including passenger terminals that handle domestic ferries and any passenger vessel terminal serving vessels carrying more than 150 passengers. This is what the Coast Guard calls a layered approach to maritime security, where the individual terminal and facility security plans are essential elements and components of the larger area security plans. The Coast Guard will also issue maritime security directives that can be issued to regulated industry based on the prevailing threat to impose specific measures designed to address that specific threat.

In addition, the Coast Guard will evaluate a foreign country's overall compliance with the International Ship and Port Facility Security Code, an international agreement signed in December 2002. The Coast Guard has already begun visits to foreign countries and plans to continue providing assistance with interpretation of the International Code and to help international governments and private firms understand that everything possible must be done to ensure maritime transportation system security with minimal disruption to global trade and the U.S. economy. The Coast Guard will use the information gained from these visits to help improve U.S. security practices and to determine if additional security measures will be required for vessels arriving in the United States from other countries.

Photo courtesy of the Port of Seattle

All told, our Marine Transportation System contributes over $1 trillion to the U.S. gross domestic product, the system is vital, though still vulnerable to terrorist activity. Here, ships at the Port of Seattle's Terminal 5 are loaded with cargo containers.

Summary

Time is extremely short, and much work remains to be done to meet the impending Maritime Transportation Security Act and ISPS Code entry-into-force date of July 1, 2004. The security and economic consequences for the world's global economy are too high if we fail to meet this challenge. The United States is struggling to fully implement the ISPS Code but is confident that it will make it. Maritime transportation security stakeholders that have not yet begun to work to implement the ISPS Code may get caught short. This is a collective risk that we share, and improved security can only be realized if we all do our part. According to a recent news article in *The Seattle Times*, Secretary Tom Ridge of the Department of Homeland Security is quoted as saying that "the federal government will issue about $4.4 billion in grants to local governments for security this year, including port security, but our job now is to make the business case to the private companies that they need to start picking up the tab." We must work with all due speed to complete the required assessments and to develop meaningful security plans. Failure is not an option as we all struggle to enhance the security of our vital and vulnerable maritime transportation system.

Gerald P. Fleming is the Communications Director for Maritime Security, Anteon Corporation.